Communications Security (COMSEC)

1. General

General requirements and standard procedures for the operation of DOE and DOE contractor accounts are set forth in NSA COMSEC publications and DOE M 200.1-1 Telecommunications Security Manual. Communications security (COMSEC) policy is governed by the DOE COMSEC Central Office of Records (COR) and the National Security Agency (NSA). COMSEC information is considered especially sensitive because of the need to safeguard U.S. cryptographic principles, methods, and material against exploitation, and to protect the classified information encrypted in U.S. crypto systems.

The protection policy for national telecommunications contains two major elements:

1. Government classified information relating to national defense and foreign relations shall be transmitted only by secure means.
2. Unclassified information transmitted by and between Government agencies and contractors that would be useful to an adversary should be protected.

All classified information transmitted at BNL must be secured by using cryptographic equipment or protected distribution systems approved by the National Security Agency. Unclassified but sensitive information that would be useful to an adversary will be protected by the use of encrypted communications whenever possible.

2. Appointment of COMSEC Personnel

COMSEC Control Officer - Person designated by proper authority to be responsible for the oversight and operation of a COMSEC account.

COMSEC Custodian - Person designated by proper authority to be responsible for the receipt, transfer, accounting, safeguarding and destruction of COMSEC material assigned to a COMSEC account.

The COMSEC Control Officer and the COMSEC Custodian are appointed in writing by the BNL Security Manager. Their responsibilities are listed in DOE M 200.1-1 Telecommunications Security Manual, Chapter 3.

COMSEC Control Officer - L. Congemi X-8451

COMSEC Custodian – L. Congemi X-8451

3. Acquisition of COMSEC Material

All accountable COMSEC material, with the exception of STU-III keying material, shall be controlled through the DOE COMSEC Material Control System (CMCS). STU-III keying material shall be controlled through the NSA Electronic Key Management System (EKMS). The guidelines, limitations, and procedures for acquisition of COMSEC material and certain crypto related equipment and supplies are applicable to all DOE organizations and DOE contractors except where other arrangements are specifically authorized by the Engineering and Assessment Division, Office of the Associate CIO for Cyber Security. All COMSEC equipment sent to BNL will be initially received by the COMSEC Custodian for processing and distribution to users.

4. Distribution of Material

Distribution of COMSEC material and accountable crypto-related material shall be conducted through the COMSEC distribution channel, and in accordance with the procedures set forth in DOE M 200.1-1.

COMSEC and CRYPTO material shall be transferred only between COMSEC Custodians, Subcustodians, and their alternates using the packaging, marking, shipping, inspection and receipting procedures prescribed in DOE M 200.1-1. Distribution is based on operational necessity and a need-to-know basis.

5. Accounting for Material

All accountable COMSEC material, with the exception of STU-III keying material, which is controlled through the EKMS, is entered into the DOE COMSEC Material Control System (CMCS) at the time of origin. Other COMSEC Materials, identified by "TSEC", "CE", or "E" designators, essential to secure communications, are entered into the CMCS unless an exemption has been granted by the Engineering and Assessment Division, Office of the Associate CIO for Cyber Security.

It is the responsibility of each individual charged with the custody of COMSEC material to know the exact location of each item entrusted to his/her care, and the general purpose for which it is being used at all times. COMSEC material of all classifications shall be accounted for by means of the COMSEC accounting system, and shall be exempt from other accounting systems, including "Top Secret" control document systems and property management systems.

6. COMSEC Audit

The Office of Cyber Security will conduct a COMSEC audit and crypto facility COMSEC survey pertaining to crypto security, transmission security, COMSEC accounting, and COMSEC operation of communications centers/COMSEC accounts on a biennial basis, or more often if required. Notification of the audit and crypto facility survey will be sent to the responsible field officer prior to the scheduled visit. Copies of the COMSEC audit and survey report with a statement of proposed corrective actions, if any, will be furnished to the responsible field officer. The COMSEC Custodian is also provided a copy of the formal report, which should be retained in the COMSEC files.

7. BNL COMSEC Account Operations

Brookhaven National Laboratory's COMSEC policies are consistent with the criteria set forth in DOE M 200.1-1, Telecommunications Security Manual, dated March 15, 1997. These requirements and procedures apply to all COMSEC accounts, including sub-accounts, and personnel who control or access COMSEC equipment and process classified information through a crypto device. All COMSEC operations are controlled through the appropriate facility Custodian or their alternate. Initial training and annual refreshers are required for all custodians and users.

Locations:

- Building 50 - The Safeguards and Security Division controls the availability of B/50 COMSEC equipment for classified telephone communication and receipt/transmission of classified matter. This system is also available for use after normal business hours. For use during normal business hours contact Lisa Congemi at X-8451, or Susan Rackett at X-5149. After normal business hours, contact Police Headquarters at X-2238.

- Building 197C – The Nonproliferation and National Security Department controls the availability of B/97C COMSEC equipment for classified telephone communication and receipt/transmission of classified matter during normal business hours. This system is not available after business hours. Contact Susan Carlsen at X-7647.

- Building 801 - The Counterintelligence Office controls the availability of B/801 COMSEC equipment for use by Counterintelligence personnel. During an emergency situation if no other secure communications is available, the CI office may authorize the use of B/801 COMSEC equipment by non CI Laboratory personnel. During normal operations, this system is not available after business hours. Contact Sharon Jones at X-2493 or Gary Gross at X-2234.

8. Definitions

Communications Security (COMSEC) - Measures and controls taken to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. Communications security includes crypto security, transmission security, emissions security, and physical security of COMSEC material.

COMSEC Equipment - Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and subsequently, by reconverting such information to its original form for authorized recipients; also equipment designed specifically to aid in, or as an essential element of the conversion process. COMSEC equipment includes crypto equipment, crypto ancillary equipment, crypto production equipment, and authentication equipment.

COMSEC Material - All documents, aids, devices, or equipment (including CRYPTO) associated with the security and authentication of telecommunications.

COMSEC Material Control System (CMCS) - Logistics and accounting system, through which COMSEC material is distributed, controlled and safeguarded. Included are the COMSEC Central Office of Record (COR), crypto logistic depots, and COMSEC accounts.

CRYPTO - Marking or designator identifying all COMSEC keying material used to secure or authenticate telecommunications carrying classified or sensitive U.S. Government or U.S. Government-derived information. When written in lower case, crypto and crypt are abbreviations for cryptographic.

Data Encryption Standard (DES) - Cryptographic algorithm designed for the protection of unclassified data and published by the National Institute of Standards and Technology (NIST) in Federal Information Processing Standard Publication 46.

Emissions Security (TEMPEST) - Protection resulting from all measures taken to deny unauthorized persons information of value derived from intercept and analysis of compromising emanations from crypto-equipment, AIS, and telecommunications systems.

Keying Material - Key, code, or authentication information in physical or magnetic form.

Physical Security- The component of COMSEC which results from all physical measures necessary to safeguard COMSEC material and information from both physical and visual unauthorized access.

Protected Distribution System (PDS) - Wireline or fiber-optic telecommunications system that includes adequate acoustical, electrical, electromagnetic, and physical safeguards so that it may be used for the transmission of unencrypted classified information.

Reportable COMSEC Occurrence - All deviations from rules of communications security (both personnel and physical) or any occurrence, which may detrimentally affect the security of COMSEC information or encrypted communications.

Secure Telephone Unit (STU) - Telecommunications security nomenclature, e.g., STU-III, KY-70, referring to a telephone like device utilized for secure communications. Also referred to as a Security Voice System.